Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Newly Amended) A method for securing a data object, comprising:
providing an openly accessible [a] data object comprising digital data and file format information;
embedding independent data into the openly accessible data object; and
scrambling the openly accessible data object to degrade the openly accessible data object to a predetermined signal quality level where at least a portion of the independent data can be decoded from the scrambled openly accessible data object.

2. (original) The method of claim 1, further comprising the step of performing the steps of embedding and scrambling until a predetermined condition is met.

3. (Newly Amended) The method of claim 2, wherein the predetermined condition comprises reaching a desired signal quality level of the openly accessible data object.

4. (Newly Amended) The method of claim 1, further comprising the steps of:
descrambling the data object to upgrade the openly accessible data object to a predetermined signal quality level; and
decoding the embedded independent data.

5. (original) The method of claim 4, further comprising the step of performing the steps of embedding and scrambling until a predetermined condition is met.

6. (Newly Amended) The method of claim 5, wherein the predetermined condition comprises reaching a desired signal quality level of the openly accessible data object.

7. (original) The method of claim 1, wherein the predetermined signal quality level is selected from the group consisting of telephone quality, radio quality, MP3 quality, and CD quality.

8. (original) The method of claim 1, wherein the predetermined signal quality level is selected from the group consisting of NTSC quality, QuickTime quality, Macrovision quality, satellite quality, high definition quality, and DVD quality.

9. (original) The method of claim 1, wherein the independent data comprises authenticatable data.

10. (original) The method of claim 9, wherein the authenticatable data comprises a robust open watermark.

11. (previously presented) The method of claim 4, wherein the step of decoding the embedded independent data comprises using a public key to decode the independent data.

12. (Newly Amended) The method of claim 1, wherein the openly accessible data object comprises at least one of digital music, video, and at least one image.

13. (Newly Amended) The method of claim 1, further comprising the step of:
scrambling the independent data before the embedding step so that the embedding step embeds the scrambled independent data into the openly accessible data object.

14. (Newly Amended) A method for distributing a data signal, comprising:
providing a data signal comprising digital data and file format information;
selecting a first scrambling technique to apply to the data signal;
scrambling the data signal using the first scrambling technique, resulting in a first-level degraded data signal;
creating a first descrambling key for the first-level degraded data signal based on the first scrambling technique where at least a portion of embedded data can be decoded from the scrambled digital signal.;
selecting a second scrambling technique to apply to the first-level degraded data signal;
scrambling the first-level degraded data signal using a second scrambling technique, resulting in a second-level degraded data signal; and
creating a second descrambling key for the second-level degraded data signal based on the second scrambling technique where at least a portion of embedded data can be decoded from the scrambled digital signal.

15. (original) The method of claim 14, further comprising:
associating a first payment level with the data signal;
associating a second payment level with the first-level degraded data signal; and
associating a third payment level with the second-level degraded data signal.

16. (previously presented) The method of claim 15, further comprising:
selecting a payment level; and
applying at least one of the descrambling keys to the second-level degraded data signal, resulting in the associated data signal.

17. (original) The method of claim 14, wherein at least one of the first scrambling technique and the second scrambling technique comprises manipulation of the file format information.

18. (original) The method of claim 14, wherein at least one of the first scrambling technique and the second scrambling technique comprises a cryptographic cipher.

19. (previously presented) The method of claim 14, wherein the data signal quality levels are selected from the group consisting of CD quality, MP3 quality, radio quality, and telephone quality.

20. (previously presented) The method of claim 14, wherein the predetermined data signal quality level is selected from the group consisting of NTSC quality, QuickTime quality, Macrovision quality, satellite quality, and DVD quality.

21. (Newly Amended) A method for distributing a data object, comprising:
providing a data object comprising digital data and file format information;
encoding independent authentication data into the data object; [and]
manipulating the file format information based on at least one signal characteristic of the data object where at least a portion of the independent authentication data can be decoded from the manipulated data object; [.]and
distributing the manipulated data object where access to the manipulated data object in not conditional.

22. (original) The method of claim 21, wherein the independent authentication data is stegnographically encoded into the data object.

23. (original) The method of claim 21, wherein the independent authentication data comprises a robust open watermark.

24. (original) The method of claim 21, wherein the at least one signal characteristic of the data object comprises file format information.

25. (original) The method of claim 21, further comprising the step of:
generating at least one cryptographic key based on a result of the manipulation of the file format information.

26. (original) The method of claim 25, wherein the step of generating at least one cryptographic key based on a result of the manipulation of the file format information comprises:
selecting at least one of a plurality of signal characteristics of the data format; and
ciphering the results of the order of steps of signal characteristic selection.

27. (original) The method of claim 21, wherein the step of manipulating the file format information based on at least one signal characteristic of the data object comprises multiple step manipulation, and an order of the multiple step manipulation is ciphered to generate a predetermined key.

28. (original) The method of claim 21, wherein the steps of encoding independent authentication data into the data object and manipulating the file format information based on at least one signal characteristic of the data object comprise multiple step encoding and manipulation, and an order of the multiple steps is ciphered to generate a predetermined key.

29. (original) The method of claim 21, further comprising:
generating at least one cryptographic key having a logical relationship with the manipulation of the file format information and the steganographic encoding method.

30. (previously presented) The method of claim 21, further comprising:
generating an authorization key that is dependent on a public key and a private key;

wherein the authorization key is further dependent on at least one of a time, a channel, and an object.

31. (Newly Amended) A method for distributing data signals, comprising:
embedding independent data into a data object;
scrambling the data object where at least a portion of the independent data can be decoded from the scrambled data object;
distributing the scrambled data object;
distributing at least one predetermined key that enables access to the data object, the embedded independent data, or both the data object and the embedded independent data;
decoding at least a portion of the independent data from the scrambled data object with the predetermined key; and
descrambling the scrambled data object with the predetermined key.

32. (original) The method of claim 31, wherein the independent data comprises payment information.

33. (original) The method of claim 31, wherein the independent data comprises authentication information.

34. (original) The method of claim 31, wherein the independent data comprises a one-way hash.

35. (original) The method of claim 31, wherein the independent data comprises a digital signature.

36. (original) The method of claim 31, wherein the independent data comprises a time stamp.

37. (original) The method of claim 31, wherein the steps of embedding independent data into a data object and scrambling the data object each has a logical relationship with the generation of the predetermined key.

38. (original) The method of claim 31, wherein the steps of embedding independent data into a data object and scrambling the data object each has a logical relationship with the generation of the predetermined key and a communications channel for which the data signal is being prepared.

39. (original) The method of claim 31, wherein the step of descrambling the scrambled data object comprises:
initiating the transmission of a recipient public key from an intended recipient of the data object to a sender of the data object; and
initiating the transmission of a sender session key from the sender to the recipient to initiate descrambling of the embedded independent data

40. (original) The method of claim 31, wherein the step of descrambling the scrambled data object comprises:
initiating a session key-based exchange between a sender and receiver;
wherein the session key is dependent on at least one of a channel, a time, and a data object

41. (original) The method of claim 31, wherein the step of descrambling the scrambled data object comprises:
initiating a session key-based exchange between a sender and a receiver that is a timing based timing mechanism.

42. (original) The method of claim 31, wherein the step of descrambling the scrambled data object comprises:
initiating a pooling of similar session keys.

43. (original) The method of claim 31, wherein the step of descrambling the scrambled data object comprises:
logically associating a signal quality with a predetermined estimation of a bandwidth requirement for the session.

44. (original) The method of claim 31, wherein the step of descrambling the scrambled data object comprises:
logically associating a signal quality with a bandwidth allocation model.

45. (original) The method of claim 31, wherein the step of descrambling the scrambled data object comprises:
logically associating a signal quality with a signal quality parameter.

46. (original) The method of claim 31, wherein the step of descrambling the scrambled data object comprises:
updating a signal quality of the data object based on an approval of the session keys by the originating data signal server

47. (original) The method of claim 31, wherein the step of scrambling the data object comprises:
manipulating file format information of the data object.

48. (original) The method of claim 31, wherein the step of scrambling the data object comprises:
scrambling the data object with a cryptographic cipher.

49. (Newly Amended) A method for data signal distribution comprising:
applying a steganographic technique for embedding independent data into the data signal;

applying a scrambling technique selected from the group consisting of file format manipulation and partial encryption where at least a portion of the embedded independent data can be decoded from the scrambled data signal; and

generating a predetermined key based on the embedding and scrambling steps.

50. (original) The method of claim 49, wherein the file format manipulation scrambling technique has a relationship with at least one signal characteristic of the data signal.

51. (original) The method of claim 49, wherein the partial encryption scrambling technique is unrelated to any characteristic of the data signal.

52. (original) The method of claim 49, wherein the partial encryption scrambling technique degrades a signal quality of the data signal.

53. (original) The method of claim 49, wherein the predetermined key enables descrambling of the signal.

54. (original) The method of claim 49, wherein the predetermined key is based on unique identifying information for a receiver.

55. (original) The method of claim 49, wherein the predetermined key is based on a signal quality threshold that is adjustable in at least one of a time, a frequency, and a bit depth.

56. (original) The method of claim 49, wherein the predetermined key is based on a signal quality threshold that is adjustable in at least of one of a time, a frequency, a bit depth, and a measure of payment that may be adjusted for at least one of a time, a frequency, and a bit depth.

57. (original) The method of claim 49, wherein the predetermined key is pregenerated based on at least one expected characteristic of the data signal.

58. (original) The method of claim 49, wherein the predetermined key is divisible into a plurality of discrete partial keys, each discrete partial key representing less than an entire payment for the data signal.

59. (original) The method of claim 49, wherein the predetermined key can be broken into a plurality of discrete partial keys, each discrete partial key representing less than an entire descrambled state for the data signal.

60. (Newly Amended) A method for bandwidth allocation, comprising:

presenting a plurality of openly accessible data objects to a user, each data object having a security application, where the security applications comprises embedding, scrambling, or both embedding and scrambling;

linking at least a first data object to at least one second data object;

wherein a characteristic of the first data object causes a change in the second data object.

61. (original) The method of claim 60, wherein the first data object comprises advertising.

62. (original) The method of claim 60, wherein an increased quantity of the first data object causes a signal quality level of the second data object to increase.

63. (original) The method of claim 60, wherein a signal quality level of the second data object is increased with a predetermined key.

64. (original) The method of claim 63, wherein the predetermined key comprises at least one session key.

65. (original) The method of claim 64, wherein the at least one session key adjusts a payment for the second data object.

66. (Newly Amended) A system for securing data within a data object, comprising:
an embedder that embeds independent data into [a] an openly accessible data object; [and]
a scrambler that scrambles the openly accessible data object to degrade the openly accessible data object to a predetermined signal quality level.
a decoder that can decode at least a portion of the independent data from the scrambled openly accessible data object.

67. (original) The system of claim 66, further comprising:
a descrambler that descrambles the data object to upgrade the data object to a predetermined signal quality level; and
a decoder that decodes the embedded independent data.

68. (Newly Amended) A system for distributing a data signal, comprising:
a first selector that selects a first scrambling technique to apply to the data signal;
a first scrambler that scrambles the data signal using the first scrambling technique, resulting in a first-level degraded data signal;
a first key creator that creates a first descrambling key for the first-level degraded data signal based on the first scrambling technique where at least a portion of embedded data can be decoded from the scrambled digital signal;
a second selector that selects a second scrambling technique to apply to the first-level degraded data signal;
a second scrambler that scrambles the first-level degraded data signal using a second scrambling technique, resulting in a second-level degraded data signal; and
a second key creator that creates a second descrambling key for the second-level degraded data signal based on the second scrambling technique where at least a portion of embedded data can be decoded from the scrambled digital signal.